REMARKS

The present application and its claims are directed to a mobile application security system and method.

PRIOR ART REJECTIONS

In response to the Examiner's rejection of Claims 1-8 under 35 U.S.C. 102(a) as being anticipated by Jansen et al., NIST Special Publication 800-19- Mobile Application Security (hereinafter "Jansen"), Applicant respectfully traverses the rejection. In particular, the claims are not anticipated by Jansen, for the reasons set forth below, and early allowance of the claims is respectfully requested.

Claims 1, 5, 9 and 12

Claim 1 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer" as set forth in the claim. To support his rejection, the Examiner cites to pages 18-19. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central security enforcement node. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central security enforcement node when the mobile application is communicated from a first node to a second node.

Section 4.2 of Jansen (on pages 18-19) describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or

suggest a system with a central computer that performs security monitoring. Thus, Jansen does not teach this element of Claim 1.

Furthermore, Claim 1 is allowable over Jansen at least because Jansen does not disclose or suggest "wherein the security monitoring means further comprises means detecting code of the mobile application marked as immutable and means for replacing the immutable code with code known to be safe by the central computer" as recited in Claim 1. The Examiner relies on Page 10 and 18-19 of Jansen to support the rejection of these claim elements. Applicant presumes that the Examiner is relying on Section 3.2 ("Integrity") on pages 9-10 and Section 4.2 ("Protecting Agents") on pages 18-19. Neither of those sections supports the Examiner's rejection for the reasons set forth below and the rejection should be withdrawn.

Section 3.2 discusses that "The agent platform must protect agents from unauthorized modification of their code, state, and data and ensure that only authorized agents or processes carry out any modification of the shared data." See Page 9 of Jansen. Jansen goes onto explain that, "The secure operation of mobile agent systems also depends on the integrity of the local and remote agent platforms themselves." See Page 10, first paragraph. Jansen then describes how a malicious platform can disrupt the security of the mobile application system. Thus, it is clear that Jansen is talking about the desirability of the security and integrity of each host platform in a mobile agent system which indicates that the system contemplated by Jansen involves each host platform performing security operations to ensure the integrity of the system and each host platform. If Jansen disclosed the claimed system with the central computer that performs security monitoring, then the problems identified in Jansen with the security of each host computer would not exist so it is unlikely that Jansen discloses or even suggests the claimed system with the central computer with the security monitoring.

Thus, in contrast, the claimed system set forth in Claim 1 does not require any host platform security or integrity since the security of the mobile application and the mobile application system is monitored by the central computer as the mobile application passes through the central computer. Thus, Section 3.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring wherein the central computer comprises means detecting code of the mobile application marked as immutable and means for replacing the immutable code with code known to be safe by the central computer.

Section 4.2 of Jansen describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform (similar to the system described in Section 3.2 above) performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring wherein the central computer comprises means detecting code of the mobile application marked as immutable and means for replacing the immutable code with code known to be safe by the central computer. Therefore, Jansen does not disclose these elements of Claim 1 and Claim 1 is allowable over Jansen.

New Claim 9, that depends from Claim 1, is allowable over Jansen for at least the same reason as Claim 1. Furthermore, Jansen does not disclose or suggest the claimed "means for inspecting the access control list of the mobile application to determine if the code of the mobile application is marked as immutable."

Claim 5 is allowable for at least the same reason as Claim 1 and Claim 12 is allowable for at least the same reasons as Claim 9 above.

Claims 2, 6, 10 and 13

Claim 2 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer" as set forth in the claim. To support his rejection, the Examiner cites to pages 18-19. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central security enforcement node. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central

security enforcement node when the mobile application is communicated from a first node to a second node.

Section 4.2 of Jansen (on pages 18-19) describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring. Thus, Jansen does not teach this element of Claim 2. Thus, Jansen does not teach this element of Claim 2.

Furthermore, Claim 2 is allowable over Jansen at least because Jansen does not disclose or suggest "wherein the security monitoring means further comprises means for detecting state data marked as immutable and means for replacing the immutable state data with state data known to be safe by the central computer" as recited in Claim 2. The Examiner relies on Page 10 and 18-19 of Jansen to support the rejection of these claim elements. Applicant presumes that the Examiner is relying on Section 3.2 ("Integrity") on pages 9-10 and Section 4.2 ("Protecting Agents") on pages 18-19. Neither of those sections supports the Examiner's rejection for the reasons set forth below and the rejection should be withdrawn.

Section 3.2 discusses that "The agent platform must protect agents from unauthorized modification of their code, state, and data and ensure that only authorized agents or processes carry out any modification of the shared data." See Page 9 of Jansen. Jansen goes onto explain that, "The secure operation of mobile agent systems also depends on the integrity of the local and remote agent platforms themselves." See Page 10, first paragraph. Jansen then describes how a malicious platform can disrupt the security of the mobile application system. Thus, it is clear that Jansen is talking about the desirability of the security and integrity of each host platform in a mobile agent system which indicates that the system contemplated by Jansen involves each host platform performing security operations to ensure the integrity of the system and each host platform. If Jansen disclosed the claimed system with the central computer that performs security monitoring, then the problems identified in Jansen with the security of each host

computer would not exist so it is unlikely that Jansen discloses or even suggests the claimed system with the central computer with the security monitoring.

Thus, in contrast, the claimed system set forth in Claim 1 does not require any host platform security or integrity since the security of the mobile application and the mobile application system is monitored by the central computer as the mobile application passes through the central computer. Thus, Section 3.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring wherein the central computer comprises means detecting state data of the mobile application marked as immutable and means for replacing the immutable code with state data known to be safe by the central computer.

Section 4.2 of Jansen describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform (similar to the system described in Section 3.2 above) performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring wherein the central computer comprises means detecting state data of the mobile application marked as immutable and means for replacing the immutable state data with state data known to be safe by the central computer. Therefore, Jansen does not disclose these elements of Claim 2 and Claim 2 is allowable over Jansen.

Claim 10 is allowable for at least the same reasons as Claim 2 and further allowable for at least the same reasons as Claim 9 above.

Claim 6 is allowable for at least the same reason as Claim 2 and Claim 13 is allowable for at least the same reason as Claim 10.

Claims 3, 7, 11 and 14

Claim 3 is not anticipated by Jansen for at least the reason that Jansen does not disclose "the central computer further comprising means for monitoring the security of the mobile application as it jumps between the host computers wherein when the mobile application is communicated from a first host to a second host, it passes through the central computer" as set

forth in the claim. To support his rejection, the Examiner cites to pages 18-19. At pages 18-19, Jansen, citing to the Jumping Beans system, describes a system with a secure central host and a decentralized system called Aglets wherein each host is capable of rejecting an agent from a platform that is not a trusted peer. Clearly, the Aglets system does not have a central security enforcement node. The Jumping Beans systems as described in the Jansen article, has a secure central host, but Jansen does not describe that the Jumping Beans system performs the operations set forth in the claim, namely the security monitoring of the mobile application at the central security enforcement node when the mobile application is communicated from a first node to a second node.

Section 4.2 of Jansen (on pages 18-19) describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring. Thus, Jansen does not teach this element of Claim 3. Thus, Jansen does not teach this element of Claim 3.

Furthermore, Claim 3 is allowable over Jansen at least because Jansen does not disclose or suggest "wherein the security monitoring means further comprises means for detecting the itinerary marked as immutable and means for replacing the immutable itinerary data with itinerary data known to be safe by the central computer" as recited in Claim 3. The Examiner relies on Page 10 and 18-19 of Jansen to support the rejection of these claim elements. Applicant presumes that the Examiner is relying on Section 3.2 ("Integrity") on pages 9-10 and Section 4.2 ("Protecting Agents") on pages 18-19. Neither of those sections supports the Examiner's rejection for the reasons set forth below and the rejection should be withdrawn.

Section 3.2 discusses that "The agent platform must protect agents from unauthorized modification of their code, state, and data and ensure that only authorized agents or processes carry out any modification of the shared data." See Page 9 of Jansen. Jansen goes onto explain that, "The secure operation of mobile agent systems also depends on the integrity of the local and

remote agent platforms themselves." See Page 10, first paragraph. Jansen then describes how a malicious platform can disrupt the security of the mobile application system. Thus, it is clear that Jansen is talking about the desirability of the security and integrity of each host platform in a mobile agent system which indicates that the system contemplated by Jansen involves each host platform performing security operations to ensure the integrity of the system and each host platform. If Jansen disclosed the claimed system with the central computer that performs security monitoring, then the problems identified in Jansen with the security of each host computer would not exist so it is unlikely that Jansen discloses or even suggests the claimed system with the central computer with the security monitoring.

Thus, in contrast, the claimed system set forth in Claim 1 does not require any host platform security or integrity since the security of the mobile application and the mobile application system is monitored by the central computer as the mobile application passes through the central computer. Thus, Section 3.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring wherein the central computer comprises means detecting itinerary data of the mobile application marked as immutable and means for replacing the immutable itinerary data with itinerary data known to be safe by the central computer.

Section 4.2 of Jansen describes the problem of protecting an agent which "stems from the inability to effectively extend the trusted environment of an agent's home platform to other agent platforms." See page 18, second paragraph. For the reasons that the claimed system has the central computer through which the mobile application is communicated, the claimed system does not suffer from this drawback highlighted by Jansen. In fact, this section makes it clear that Jansen is describing a mobile application system in which each host platform (similar to the system described in Section 3.2 above) performs its own security. Thus, Section 4.2 of Jansen does not in any way disclose or suggest a system with a central computer that performs security monitoring wherein the central computer comprises means for detecting itinerary data of the mobile application marked as immutable and means for replacing the immutable itinerary data with itinerary data known to be safe by the central computer. Therefore, Jansen does not disclose these elements of Claim 3 and Claim 3 is allowable over Jansen.

New Claim 11, which depends from Claim 3 is allowable for at least the same reasons as Claim 9 above. Furthermore, Claim 7 is allowable for at least the same reason as Claim 3 and Claim 14 is allowable for at least the same reason as Claim 11.

New Claims 15 and 16

New Claim 15 is allowable over the prior art at least because the claims recites "receiving a mobile application at a central computer each time the mobile application is jumping between a first host and a second host." For the reasons set forth above, this element is not disclosed by Jansen.

Furthermore, Jansen does not disclose the combination of the security monitoring elements (or steps in Claim 15.) In particular, Claim 15 recites the combination of a saving step, a stripping step, a replacing step and a saving step that are not shown in Jansen. Furthermore, Jansen does not disclose the details of each of these steps. Therefore, Claim 15 is allowable. Claim 16 is allowable for at least the same reasons as Claim 15.

CONCLUSION

In view of the above, it is respectfully submitted that Claims 1-16 are allowable over the prior art cited by the Examiner and early allowance of these claims and the application is respectfully requested.

The Examiner is invited to call Applicant's attorney at the number below in order to speed the prosecution of this application.

The Commissioner is authorized to charge any deficiencies in fees and credit any overpayment of fees to Deposit Account No. 07-1896.

Respectfully submitted,

GRAY CARY WARE & FREIDENRICH LLP

Dated: March 31, 2004

By _____
Timothy W. Lohse
Reg. No. 35,255
Attorney for Applicant

GRAY CARY WARE & FREIDENRICH
2000 University Avenue
East Palo Alto, CA 94303
Telephone: (650) 833-2055

Gray Cary\EM\7162213.1
1010722-991102

Gray Cary\EM\7162213.1
1010722-991102